UNITED NATIONS

GENERAL
ASSEMBLY

Distr.
LIMITED

A/CN.9/WG.IV/WP.71
31 December 1996

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on
Electronic Commerce
Thirty-first session
New York, 18-28 February 1997

PLANNING OF FUTURE WORK ON ELECTRONIC COMMERCE: DIGITAL SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES

Note by the Secretariat

CONTENTS

	Paragraphs	Page
INTRODUCTION	1-11	3
I. GENERAL REMARKS ON DIGITAL SIGNATURES	12-45	6
A. Functions of signatures	12-13	6
B. Digital signatures and other electronic signatures	14-45	6
1. Electronic signatures relying on techniques other than public-key cryptography	15-17	6
2. Digital signatures relying on public-key cryptography	18-45	7
(a) Technical notions and terminology	18-27	7
(i) Cryptography	18-20	7
(ii) Public and private cryptographic keys	21-22	8
(iii) "Hash function"	23	9
(iv) Digital signature	24-25	9
(v) Verification of digital signature	26-27	9
(b) Public key infrastructure (PKI) and certification authorities	28-44	10
(i) Public key infrastructure (PKI)	33-35	11
(ii) Certification authorities	36-44	12
(c) Summary of the digital signature process	45	14

		Paragraphs	Page
II.	LEGAL ISSUES AND POSSIBLE PROVISIONS TO BE CONSIDERED IN UNIFORM RULES ON DIGITAL SIGNATURES	46-76	15
	A. Scope of work	46-48	15
	B. Sphere of application of uniform rules on digital signatures and general provisions	49-51	16
	C. Specific legal issues and draft provisions on digital signatures	52-76	16
	1. Definitions	52-60	16
	(a) Digital signature	55-56	17
	(b) Authorized certification authorities	57-58	18
	(c) Certificates	59-60	18
	2. Signature by natural and legal persons	61-63	19
	3. Attribution of digitally signed messages	64-65	20
	4. Revocation of certificates	66-67	21
	5. Register of certificates	68-69	21
	6. Liability	70-72	22
	7. Issues of cross-certification	73-75	23
	8. Relations between users and certification authorities	76	24
III.	INCORPORATION BY REFERENCE	77-93	25
	A. Previous discussion	77-79	25
	B. Possible need for uniform rules on incorporation by reference	80-90	26
	1. Traditional rules developed in a paper-based environment	81-83	26
	(a) Incorporation by reference	81-82	26
	(b) "Battle of forms"	83	27
	2. Issues raised in an electronic commerce environment	84-90	27
	(a) Widespread use of incorporation by reference	84-87	27
	(b) Accessibility of incorporated text	88-90	28
	C. Possible provision	91-93	29

INTRODUCTION

1. Upon adoption of the UNCITRAL Model Law on Electronic Commerce, the Commission, at its twenty-ninth session, proceeded with a discussion of future work in the field of electronic commerce, based on a preliminary debate held by the Working Group on Electronic Data Interchange at its thirtieth session (A/CN.9/421, paras. 109-119). It was generally agreed that UNCITRAL should continue its work on the preparation of legal standards that could bring predictability to electronic commerce, thereby enhancing trade in all regions.

2. New proposals were made as to possible topics and priorities for future work. One proposal was that the Commission should start preparing rules on digital signatures. It was stated that the establishment of digital signature laws, together with laws recognizing the actions of "certifying authorities" (hereinafter referred to as "certification authorities"), or other persons authorized to issue electronic certificates or other forms of assurances as to the origin and attribution of messages "signed" digitally, was regarded in many countries as essential for the development of electronic commerce. It was pointed out that the ability to rely on digital signatures would be a key to the growth of contracting as well as the transferability of rights to goods or other interests through electronic media. In a number of jurisdictions, new laws governing digital signatures were currently being prepared. It was reported that such law development was already non-uniform. Should the Commission decide to undertake work in that area, it would have an opportunity to harmonize the new laws, or at least to establish common principles in the field of electronic signatures, and thus to provide an international infrastructure for such commercial activity.

3. Considerable support was expressed in favour of the proposal. It was generally felt, however, that, should the Commission decide to undertake work in the field of digital signatures through its Working Group on Electronic Data Interchange, it should give the Working Group a precise mandate. It was also felt that, since it was impossible for UNCITRAL to embark on the preparation of technical standards, care should be taken that it would not become involved in the technical issues of digital signatures. It was recalled that the Working Group, at its thirtieth session, had recognized that work with respect to certification authorities might be needed, and that such work would probably need to be carried out in the context of registries and service providers. However, the Working Group had also felt that it should not embark on any technical consideration regarding the appropriateness of using any given standard (A/CN.9/421, para. 111). A concern was expressed that work on digital signatures might go beyond the sphere of trade law and also involve general issues of civil or administrative law. It was stated in response that the same was true of the provisions of the Model Law and that the Commission should not shy away from preparing useful rules for the reason that such rules might also be useful beyond the sphere of commercial relationships.

4. Another proposal, based on the preliminary debate held by the Working Group, was that future work should focus on service providers. The following were mentioned as possible issues to be considered with respect to service providers: the minimum standards for performance in the absence of party agreement; the scope of assumption of risk by the end parties; the effect of such rules or agreements on third parties; allocation of the risks of interlopers' or other unauthorized actions; and the extent of mandatory warranties, if any, or other obligations when providing value-added services (see A/CN.9/421, para. 116).

5. It was widely felt that it would be appropriate for UNCITRAL to examine the relationship between service providers, users and third parties. It was said that it would be very important to direct such an effort towards the development of international norms and standards for commercial conduct in the field, with the intent of supporting trade through electronic media, and not have as a goal the establishment of a regulatory regime for service providers, or other rules which could create costs unacceptable for market applications of EDI (see A/CN.9/421, para. 117). It was also felt, however, that the subject-matter of service providers might be too broad and cover too many different factual situations to be treated as a single work item. It was generally agreed that issues pertaining to service providers could appropriately be dealt with in the context of each new area of work addressed by the Working Group.

6. Yet another proposal was that the Commission should begin work on the preparation of the new general rules that were needed to clarify how traditional contract functions could be performed through electronic commerce. Uncertainties were said to abound as to what "performance", "delivery" and other terms meant in the context of electronic commerce, where offers and acceptances and product delivery could take place on open computer networks across the world. The rapid growth of computer-based commerce as well as transactions over the Internet and other systems had made that a priority topic. It was suggested that a study by the Secretariat could clarify the scope of such work. Should the Commission, after examination of the study, decide to pursue this task, one option would be to place such rules in the "Special provisions" section of the UNCITRAL Model Law on Electronic Commerce.

7. A further proposal was that the Commission should focus its attention on the issue of incorporation by reference. It was recalled that the Working Group had agreed that that topic would appropriately be dealt with in the context of more general work on the issues of registries and service providers (A/CN.9/421, para. 114). The Commission was generally agreed that the issue could be dealt with in the context of work on certification authorities.

8. After discussion, the Commission agreed that placing the issue of digital signatures and certification authorities on the agenda of the Commission was appropriate, provided that it was used as an opportunity to deal with the other topics suggested by the Working Group for future work. It was also agreed as to a more precise mandate for the Working Group that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference.

9. The Commission requested the Secretariat to prepare a background study of the issues of digital signatures and service providers, based on an analysis of laws currently being prepared in various countries. On the basis of that study, the Working Group should examine the desirability and feasibility of preparing uniform rules on the above-mentioned topics. It was agreed that work to be carried out by the Working Group at its thirty-first session could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the scope of the uniform rules to be prepared. In view of the broad scope of activities covered by the UNCITRAL Model Law on Electronic Commerce and by possible future work in the area of electronic commerce, it was decided that the Working Group

on Electronic Data Interchange would be renamed "Working Group on Electronic Commerce". [1/]

10. This note contains a preliminary study of the issues of digital signatures and related issues. It was prepared against the background of the UNCITRAL Model Law on Electronic Commerce, also taking into account the legislative texts recently adopted, or currently being prepared in a number of countries. Moreover, the study draws on the work of other organizations, in particular the draft Uniform International Authentication and Certification Practices being prepared by the International Chamber of Commerce (ICC) and the Digital Signature Guidelines published by the American Bar Association, and reflects the result of a meeting of an ad hoc group of experts, which brought together experts in the area of digital signatures and the Secretariat of UNCITRAL.

11. In line with the recent instructions relating to the stricter control and limitation of United Nations documents, the explanatory remarks to the draft provisions are as brief as possible. Additional explanations will be provided orally.

[1/] Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 216-224.

I. GENERAL REMARKS ON DIGITAL SIGNATURES

A. Functions of signatures

12. Article 7 of the UNCITRAL Model Law on Electronic Commerce is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Model Law, the Working Group discussed the following functions traditionally performed by hand-written signatures: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.

13. In an electronic environment, the original of a message is indistinguishable from a copy, bears no handwritten signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions. The purpose of various techniques currently available on the market or still under development is to offer the technical means by which some or all of the functions identified as characteristic of hand-written signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

B. Digital signatures and other electronic signatures

14. In discussing the desirability and feasibility of preparing uniform legal rules for digital signatures, and with a view to assisting the Commission in its consideration of the scope of such possible uniform rules, the Working Group may wish to examine various techniques currently used or still under development, the purpose of which is to provide functional equivalents to hand-written signatures and other kinds of authentication mechanisms used in a paper-based environment.

1. Electronic signatures relying on techniques other than public-key cryptography

15. It may be recalled that, alongside "digital signatures" based on public-key cryptography, which constitute the main subject-matter of this note, there exist various other devices, often referred to as "electronic signature" mechanisms, which may currently be used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of handwritten signatures. For example, certain techniques would rely on authentication through a biometrical device based on hand-written signatures. In such a device, the signer would sign manually, using a special pen, either on a computer screen or on a digital pad. The hand-written signature would then be analysed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the recipient for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analysed and stored by the biometrical device.

16. The Working Group may wish to discuss whether the scope of its work should be expanded to cover electronic signatures in general. Such work would require additional research

by the Secretariat as to the technical and legal implications of using "signature" devices relying on techniques other than public-key cryptography. In view of the availability of sufficient preliminary information as to the legal implications of digital signatures, and of the existence of draft legislation on the topic in a number countries, this note focuses on issues of digital signatures relying on public-key cryptography.

17. In discussing the desirability and feasibility of preparing uniform rules that would be applicable to both digital signatures and other forms of electronic signatures, the Working Group may wish to consider whether UNCITRAL should attempt to develop uniform rules at a level which would be intermediate between the high level of generality of the Model Law and more specific rules dealing with the particulars of one or more specific technique. In any event, consistent with media neutrality in the Model Law, the uniform rules to be developed, should they focus on digital signatures, should not discourage the use of alternative methods.

2. Digital signatures relying on public-key cryptography [2/]

(a) Technical notions and terminology

(i) Cryptography

18. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form. Digital signatures use what is known as "public key cryptography", which is often based on the use of algorithmic functions to generate two different but mathematically-related "keys" (i.e., large numbers produced using a series of mathematical formulae applied to prime numbers). One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

19. While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for confidentiality purposes. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of public policy that may involve considerations of national defence. However, the use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of encryption to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message. The Working Group may wish to consider the extent to which possible uniform rules on digital signatures should recognize the use of cryptography for authentication, as distinct from its use for confidentiality purposes.

[2/] Numerous elements of the description of the functioning of a digital signature system in this section are based on the ABA Digital Signature Guidelines, p. 8 to 17.

20. As an illustration of the reasons why different rules may be needed where encryption is used for confidentiality purposes and where it is merely used in the context of digital signatures, it is submitted that, where encryption is used to keep messages confidential, it is important in many circumstances that there be a way to recover encrypted messages if the private key is lost, in case the encrypted message has important legal, financial or public accountability value. The technology, when properly implemented, permits the issuer of the key pair to retain or recreate the missing key. However, there may be no need for a private key used to create digital signatures to be retained or recreated, and having the technical ability to do this might reduce the confidence which the users and the public at large might place in the system as a whole.

(ii) "Public and private keys"

21. The complementary keys used for digital signatures are arbitrarily termed the "private key", which is used only by the signer to create the digital signature, and the "public key", which is ordinarily more widely known and is used by a relying party to verify the digital signature. [3/] If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, for example by publication in an on-line repository or any other form of public directory where it is easily accessible. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually infeasible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is virtually impossible to determine which two prime numbers created that new, larger number. [4/] Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures.

22. It should be noted, however, that the concept of public-key cryptography does not necessarily imply the use of the above-mentioned algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as elliptic curves cryptosystems, which are often described as offering a high degree of security through the use of significantly reduced key-lengths. When discussing the issues of public-key cryptography, the Working Group may wish to recognize the extent to which public-key cryptography is being adopted in international trade. At the same time, the Working Group may wish to adopt a technically-neutral attitude, taking current technology into account without precluding future

---

[3/] The user of a private key is expected to keep the private key secret. It should be noted that the individual user does not need to know the private key. Such a private key is likely to be kept on a smart card, or to be accessible through a personal identification number or, ideally, through a biometrical identification device, e.g., through thumbprint recognition.

[4/] Certain existing standards such as the ABA Digital Signature Guidelines refer to the notion of "computational infeasibility" to describe the expected irreversibility of the process, i.e., the hope that it will be impossible to derive a user's secret private key from that user's public key. "Computationally infeasible" is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance" (ABA Digital Signature Guidelines, p. 9, note 23).

changes in the computing techniques by which key pairs are produced. Such openness to technical developments in the computer industry would, in addition, be consistent with the decision made by the Commission that it was impossible for UNCITRAL to embark on the preparation of technical standards, and that care should be taken that it would not become involved in the technical issues of digital signatures (see above, para. 3).

(iii) "Hash function"

23. In addition to the generation of key pairs, another fundamental process, generally referred to as a "hash function", is used in both creating and verifying a digital signature. A hash function is a mathematical process, based on an algorithm which creates a digital representation, or compressed form of the message, often referred to as a "message digest", or "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes termed a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

(iv) "Digital signature"

24. To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed may be referred to as the "message". Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.

25. Typically, a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if permanently disassociated from its message.

(v) Verification of digital signature

26. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key, and whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process.

27. The verification software will confirm the digital signature as "verified" if: (1) the signer's private key was used to sign digitally the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(b) Public key infrastructure (PKI) and certification authorities

28. To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. If public key encryption is to serve its intended purposes, it needs to provide a way to send keys to a wide variety of persons, many of whom are not known to the sender, where no relationship of trust has developed between the parties. To that effect, the parties involved must have a high degree of confidence in the public and private keys being issued.

29. The requested level of confidence may be present between parties who trust each other, who have dealt with each other over a period of time, who communicate on closed systems, who operate within a closed group, or who are able to govern their dealings contractually, for example, in a trading partner agreement. In a transaction involving only two parties, each party can simply communicate (by a relatively secure channel such as a courier or a secure voice telephone) the public key of the key pair each party will use. However, the same level of confidence may not be present when the parties deal infrequently with each other, communicate over open systems (e.g., the World Wide Web on the Internet), are not in a closed group, or do not have trading partner agreements or other law governing their relationships.

30. In addition, because public key encryption is a highly mathematical technology, all users must have confidence in the skill, knowledge and security arrangements of the parties issuing the public and private keys. [5/]

31. A prospective signer might issue a public statement indicating that signatures verifiable by a given public key should be treated as originating from that signer. However, other parties might be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of inadvertently trusting an imposter, or of having to disprove a false denial of a digital signature (an issue often referred to as "non-repudiation") if a transaction should turn out to prove disadvantageous for the purported signer.

32. A solution to these problems is the use of one or more trusted third parties to associate an identified signer or the signer's name with a specific public key. That trusted third party is generally referred to as a "certification authority" in most technical standards and guidelines. In

---

[5/] In situations where public and private cryptographic keys would be issued by the users themselves, such confidence might need to be provided by the certifiers of public keys.

a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a public key infrastructure (PKI).

(i) Public key infrastructure (PKI)

33. Setting up a public key infrastructure (PKI) is a way to provide confidence that: (1) a user's public key has not been tampered with and in fact corresponds to that user's private key; (2) the encryption techniques being used are sound; (3) the entities that issue the cryptographic keys can be trusted to retain or recreate the public and private keys that may be used for confidentiality encryption where the use of such a technique is authorized; (4) different encryption systems are inter-operable. To provide the confidence described above, a PKI may offer a number of services, including the following: (1) managing cryptographic keys used for digital signatures; (2) certifying that a public key corresponds to a private key; (3) providing keys to end users; (4) deciding which users will have which privileges on the system; (5) publishing a secure directory of public keys or certificates; (6) managing personal tokens (e.g., smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (7) checking the identification of end users, and providing them with services; (8) providing non-repudiation services; (9) providing time-stamping services; (10) managing encryption keys used for confidentiality encryption where the use of such a technique is authorized.

34. A public key infrastructure (PKI) is often based on various hierarchical levels of authority. For example, models considered in certain countries for the establishment of possible PKIs include references to the following levels: (1) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs, and would register subordinate certification authorities; [6/] (2) various certification authorities, placed below the "root" authority, which would certify that a user's public key actually corresponds to that user's private key (i.e., has not been tampered with); and (3) various local registration authorities, placed below the certification authorities, and receiving requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users. In certain countries, it is envisaged that notaries public might act as, or support, local registration authorities.

35. The Working Group may wish to have a general discussion of the issues of PKI. However, it is submitted that such issues may not lend themselves easily to international harmonization. The organization of a PKI may involve various technical issues, as well as issues of public policy that may better be left to each individual State. [7/] In that connection, decisions may need to be made by each State considering the establishment of a PKI, for example as to: (1) the form and number of levels of authority which should be comprised in a PKI; (2) whether only certain authorities belonging to the PKI should be allowed to issue cryptographic key pairs or whether such key pairs might be issued by the users themselves; (3)

[6/] The question as to whether a government should have the technical ability to retain or recreate private confidentiality keys may be dealt with at the level of the root authority.

[7/] However, in the context of cross-certification, the need for global interoperability requires that PKIs established in various countries should be capable of communicating with each other.

whether the certification authorities certifying the validity of cryptographic key pairs should be public entities or whether private entities might act as certification authorities; (4) whether the process of allowing a given entity to act as a certification authority should take the form of an express authorization, or "licensing", by the State, or whether other methods should be used to control the quality of certification authorities if they were allowed to operate in the absence of a specific authorization; (5) the extent to which the use of cryptography should be authorized for confidentiality purposes; and (6) whether Government authorities should retain access to encrypted information, through a mechanism of "key escrow" or otherwise. The Working Group may wish to recommend that the above-mentioned issues should not be addressed in the future work of the Commission with respect to digital signatures.

(ii) Certification authorities

36. To associate a key pair with a prospective signer, a certification authority issues a certificate, an electronic record which lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and may confirm that the prospective signer identified in the certificate holds the corresponding private key. A certificate's principal function is to bind a public key with a particular holder. A "recipient" of the certificate desiring to rely upon a digital signature created by the holder named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, assurance is provided that the digital signature was created by the holder of the public key named in the certificate, and that the corresponding message had not been modified since it was digitally signed.

37. To assure the authenticity of the certificate with respect to both its contents and its source, the certification authority digitally signs it. The issuing certification authority's digital signature on the certificate can be verified by using the public key of the certification authority listed in another certificate by another certification authority (which may but need not be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification authority must digitally sign its own certificate during the operational period of the other certificate used to verify the certification authority's digital signature.

38. A digital signature corresponding to a message, whether created by the holder of a key pair to authenticate a message or by a certification authority to authenticate its certificate, should generally be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "operational period" stated in the certificate, which is a condition of the verifiability of a digital signature.

39. To make a public key and its correspondence to a specific holder readily available for use in verification, the certificate may be published in a repository or made available by other means. Typically, repositories are on-line databases of certificates and other information available for retrieval and use in verifying digital signatures. Depending upon the implementation, retrieval of a certificate can be accomplished automatically by having the verification program directly inquire of the repository to obtain certificates as needed.

40. Once issued, a certificate may prove to be unreliable, such as in situations where the holder misrepresents its identity to the certification authority. In other circumstances, a

certificate may be reliable enough when issued but it may become unreliable sometime thereafter. If the private key is "compromised", for example through loss of control of the private key by its holder, the certificate may lose its trustworthiness or become unreliable, and the certification authority (at the holder's request or even without the holder's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the certification authority must generally publish notice of the revocation or suspension or notify persons who enquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

41. Certification authorities can conceivably be operated by Government authorities or by private sector service providers. In a number of countries, it is envisaged that, for public policy reasons, only Government entities should be authorized to operate as certification authorities. In other countries, it is considered that certification services should be open to competition from the private sector. Irrespective of whether certification authorities are operated by public entities or by private sector service providers, and of whether certification authorities would need to obtain a license to operate, there is typically more than one certification authority operating within the PKI. Of particular concern is the relationship between the various certification authorities. Certification authorities within a PKI can be established in a hierarchical structure, where some certification authorities only certify other certification authorities, which provide services directly to users. In such a structure, certification authorities are subordinate to other certification authorities. In other conceivable structures, some certification authorities may operate on an equal footing with other certification authorities. In any large PKI, there would likely be both subordinate and superior certification authorities. In any event, in the absence of an international PKI, a number of concerns may arise with respect to the recognition of certificates by certification authorities in foreign countries. The recognition of foreign certificates is often referred to as "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued.

42. Legal issues may arise with regard to cross-certifying or chaining of certificates when there are multiple security policies involved. Examples of such issues may include determining whose misconduct caused a loss, and upon whose representations the user relied. It should be noted that legal rules considered for adoption in certain countries provide that, where the levels of security and policies are made known to the users, and there is no negligence on the part of certification authorities, there should be no liability.

43. It may be incumbent upon the certification authority or the root authority to ensure that its policy requirements are met on an ongoing basis. While the selection of certification authorities may be based on a number of factors, including the strength of the public key being used and the identity of the user, the trustworthiness of any certification authority may also depend on its enforcement of certificate-issuing standards and the reliability of its evaluation of data received from users who request certificates. Of particular importance is the liability regime applying to any certification authority with respect to its compliance with the policy and security requirements of the root authority or superior certification authority, or with any other applicable requirement, on an ongoing basis.

44. The Working Group may wish to consider the following factors, to be taken into account when assessing the trustworthiness of a certification authority: (1) independence (i.e., absence of financial or other interest in underlying transactions); (2) financial resources and financial ability to bear the risk of being held liable for loss; (3) expertise in public-key technology and familiarity with proper security procedures; (4) longevity (certification authorities may be required to produce evidence of certification or decryption keys many years after the underlying transaction has been completed, in the context of a lawsuit or property claim); (5) approval of hardware and software; (6) maintenance of an audit trail and audit by an independent entity; (7) existence of a contingency plan (e.g., "disaster recovery" software or key escrow); (8) personnel selection and management; (9) protection arrangements for the certification authority's own private key; (10) internal security; (11) arrangements for termination of operations, including notice to users; (12) warranties and representations (given or excluded); (13) limitation of liability; (14) insurance; (15) inter-operability with other certification authorities; (16) revocation procedures (in cases where cryptographic keys might be lost or compromised).

(c) Summary of the digital signature process

45. The use of digital signatures usually involves the following processes, performed either by the signer or by the receiver of the digitally signed message:

(1) The user generates or is given a unique cryptographic key pair;

(2) The sender prepares a message (for example, in the form of an electronic mail message) on a computer;

(3) The sender prepares a "message digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key;

(4) The sender encrypts the message digest with the private key. The private key is applied to the message digest text using a mathematical algorithm. The digital signature consists of the encrypted message digest;

(5) The sender typically attaches or appends its digital signature to the message;

(6) The sender sends the digital signature and the (unencrypted or encrypted) message to the recipient electronically;

(7) The recipient uses the sender's public key to verify the sender's digital signature. Verification using the sender's public key proves that the message came exclusively from the sender;

(8) The recipient also creates a "message digest" of the message, using the same secure hash algorithm;

(9) The recipient compares the two message digests. If they are the same, then the recipient knows that the message has not been altered after it was signed. Even if one bit in the

message has been altered after the message has been digitally signed, the message digest created by the recipient will be different from the message digest created by the sender;

(10) The recipient obtains a certificate from the certification authority (or via the originator of the message), which confirms the digital signature on the sender's message. The certification authority is typically a trusted third party which administers certification in the digital signature system. The certificate contains the public key and name of the sender (and possibly additional information), digitally signed by the certification authority.

II. LEGAL ISSUES AND POSSIBLE PROVISIONS TO BE CONSIDERED IN UNIFORM RULES ON DIGITAL SIGNATURES

A. Scope of work

46. In deciding to place the issue of digital signatures and certification authorities on its agenda, the Commission, at its twenty-ninth session, also agreed that the issue should be used as an opportunity to deal with the other topics suggested by the Working Group for future work (see above, para. 8). Prior to entering into a discussion of the issues of digital signatures, the Working Group may wish to discuss the desirability and feasibility of limiting the scope of its work to digital signatures or of extending it to cover also other authentication mechanisms that might be currently available or soon to be developed for use in electronic commerce (see above, paras. 15-17). It may be recalled that, during the preparation of the Model Law, the Working Group was mindful of the need to establish legal rules that would not be tied to a given stage of technical and commercial development but would rather provide general principles that could be expected to remain applicable through a number of years, irrespective of possible changes in technology.

47. The widespread use of digital signatures and the risk that diverging legislative approaches be taken in various countries with respect to digital signatures may suggest that uniform legislative provisions are needed as a specific legal framework for that authentication technique. However, consistent with the media-neutral approach adopted in the preparation of the Model Law, the Working Group may wish to discuss whether it is appropriate to embark on the preparation of uniform rules that would apply to digital signatures only or whether such uniform rules should also be prepared with respect to other authentication techniques. Should the Working Group come to the conclusion that the above-mentioned risk that diverging laws be enacted in various countries suggests that the need for uniform rules applicable to digital signatures is particularly pressing, the Working Group may also wish to discuss the ways in which uniform rules on digital signatures might be drafted to avoid the risk that such uniform rules might be misinterpreted as encouraging the use of digital signatures to the detriment of competing techniques, which might also be regarded as acceptable illustrations of the concept of "reliable method" embodied in article 7 of the Model Law.

48. With respect to certification authorities, the Working Group may also wish to take into consideration that, in many practical situations, the activities of a commercial entity as a certification authority are but one aspect of a broader range of activities of that commercial entity as a service provider. The Working Group may thus wish to discuss whether uniform rules on certification authorities should be limited in scope to establishing rules of conduct

applicable only in the context of the activities of a service provider acting as a certification authority or whether it would be desirable and feasible to develop rules applicable to a wider range of activities of service providers or "trusted third parties" in electronic commerce.

B. Sphere of application of uniform rules on digital signatures and general provisions

49. This note was prepared on the assumption that possible rules on digital signatures should be directly derived from article 7 of the Model Law and should be considered as a way to provide detailed information as to the concept of a reliable "method used to identify" a person and "to indicate that person's approval" of the information contained in a data message. In considering general provisions for possible inclusion in a set of uniform rules on digital signatures, the Working Group may wish to consider more generally the relationship between such uniform rules and the UNCITRAL Model Law on Electronic Commerce. In particular, the Working Group might wish to make proposals to the Commission as to whether uniform rules on digital signatures should constitute a separate legal instrument or whether they should be incorporated in an extended version of the Model Law, for example as a separate chapter to be included in part II of the Model Law.

50. Irrespective of whether uniform rules on digital signatures are prepared as a separate instrument or as an addition to the Model Law, it is submitted that the uniform rules will need to be based on provisions along the lines of articles 1 (Sphere of application), 2(a),(c) and (e) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation), 4 (Variation by agreement), 6 (Writing) and 7 (Signature) of the Model Law. While such provisions are not expressly reproduced in this note, it should be noted that the draft uniform rules on digital signatures have been prepared by the Secretariat based on the assumption that such provisions were part of the uniform rules. In that connection, it should also be noted that provisions along the lines of articles 2, 4, 6 and 7 of the Model Law are contained in digital signature legislation being prepared in certain countries, while the Model Law is also referred to in such texts as the ABA Digital Signature Guidelines.

51. In addition to the above-mentioned provisions, the Working Group may wish to consider whether a preamble to the uniform rules should clarify the purpose of the uniform rules, namely to promote the efficient utilization of digital communication by establishing a security framework and by giving written and digital messages equal status as regards their legal effect.

C. Specific legal issues and draft provisions on digital signatures

1. Definitions

52. Laws, regulations and guidelines already implemented or currently being prepared in the area of digital signatures and certification authorities vary considerably as to the number of definitions on which they rely. Depending on the legal tradition of the enacting State, the issues of digital signatures may be dealt with mostly by way of definitions or contain no definition at all.

53. Consistent with the approach taken in the preparation of the Model Law, the Working Group may wish to consider a limited number of definitions of essential notions, such as "digital signature", "certification authorities" and "certificates".

54. The Working Group may wish to use the following possible definitions as a basis for its deliberations.

(a) Digital signature

55. "Draft article A

(1) A digital signature is a numerical value, which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine uniquely that this numerical value has been obtained with the originator's private cryptographic key.

(2) The mathematical procedures used for generating authorized digital signatures under [this Law][these Rules] are based on public-key encryption. When applied to a data message, those mathematical procedures operate a transformation of the message such that a person having the initial message and the originator's public cryptographic key can accurately determine

(a) whether the transformation was operated using the private cryptographic key that corresponds to the originator's private cryptographic key; and

(b) whether the initial message was altered after the transformation was made.

(3) A digital signature affixed to a data message is regarded as authorized if it can be verified in accordance with procedures laid down by a certification authority authorized under [this Law][these Rules].

(4) The [relevant authority in the Enacting State] shall lay down specific rules for the technical requirements to be met by digital signatures and the verification thereof."

Remarks

56. Consistent with the functional approach taken in the preparation of the Model Law, paragraphs (1) and (2) of the suggested provision focus on a brief description of the technical functions performed by public-key encryption. Paragraphs (3) and (4) reflect the principle that digital signatures are valid only if used in the context of a public-key infrastructure (PKI) implemented by public authorities.

(b) Authorized certification authorities

57. "Draft article B

(1) The ... [the enacting State specifies the organ or authority competent for authorizing certification authorities] may grant authorization to certification authorities to act in pursuance of [this Law][these Rules]. Such authorization may be revoked.

(2) The ... [the enacting State specifies the organ or authority competent to promulgate regulations with respect to authorized certification authorities] may establish rules governing the terms under which such authorizations may be granted, and promulgate regulations for the operation of certification authorities.

(3) Authorized certification authorities may issue certificates in relation to the cryptographic keys of natural and legal persons.

(4) Authorized certification authorities may offer or facilitate registration and time stamping of the transmission and reception of data messages as well as other functions regarding communications secured by means of digital signatures.

(5) The ... [the enacting State specifies the organ or authority competent to lay down specific rules with respect to the functions to be performed by authorized certification authorities] may lay down more specific rules for the functions to be performed by authorized certification authorities in connection with the issuance of certificates to individual natural or legal persons.

Remarks

58. The Working Group may wish to discuss whether the uniform rules to be prepared should expressly mention the criteria which should be taken into account when authorizing certification authorities to operate. It may be recalled that, in the context of the preparation of the Model Law, such criteria were left for inclusion in the Guide to Enactment.

(c) Certificates

59. "Draft article C

The certificate issued by an authorized certification authority, in the form of a data message or otherwise, shall indicate at least:

(a) the user's name [and address or place of business];

(b) [the day and year of birth][sufficient identification] of the user if the user is a natural person;

(c) if the user is a legal person, the name of the company and any relevant information for identifying that company;

(e) the name, address or place of business of the certification authority;

(f) the user's public cryptographic key;

(g) any necessary information indicating how verification of the user's public cryptographic key is available to the recipient of the digital signature given according to the certificate;

(h) the serial number of the certificate; and

(i) the [date of issuance and the date of expiry][validity period] of the certificate."

Remarks

60. Draft legislation on digital signature being prepared in certain countries lists some or all of the elements mentioned in draft article C as minimum information which is required to be provided in any certificate issued by a certification authority. However, consistent with the decision made by the Working Group in the preparation of the Model Law not to become involved in issued of personal data protection, the Working Group may wish to consider that, in many countries, information regarding, for example, the date of birth of a person would be protected as personal data and specific rules might govern its disclosure by electronic means.

2. Signature by legal and natural persons

61. "Draft article D

(1) Natural and legal persons may equally obtain certification of cryptographic public keys used exclusively for identification purposes.

(2) A legal person may identify a data message by affixing to that message the private cryptographic key certified for that legal person. The legal person shall only be regarded as [the originator][having approved the sending] of the message if the message is also digitally signed by the a natural person authorized to act on behalf of that legal person.

Remarks

62. The above provision is intended to clarify the conditions under which digital signatures may be applied to bind legal persons. It relies on a distinction between the two functions performed by "signature" under article 7(1)(a) of the Model Law, namely, to identify the author of a message and to indicate that person's approval of the information contained in the message. While the two functions would normally be fulfilled through the use of a single key certified for a natural person, public keys certified for legal persons would merely be used to provide assurance as to the identity of the legal person as the sender of the message. The "digital signature" of a legal person would thus be of limited effect. Any approval of the message would require, in addition to the "digital signature" (i.e., identification) of the legal person, the digital

signature of a natural person, which would both identify that person and indicate, on behalf of the legal person, the intent to approve the contents of the message.

63. While the draft provision contains a reference to "a natural person authorized to act on behalf" of a legal person, it is not intended to displace the domestic law of agency. The question as to whether the natural person did in fact and in law have the authority to act on behalf of the legal person is thus left to the appropriate legal rules outside the uniform rules.

3. Attribution of digitally signed data messages

64. "Draft article E

(1) The originator of a data message on which the originator's digital signature is affixed is bound by the content of the message in the same manner as if the message had existed in a [manually] signed form in accordance with the law applicable to the content of the message.

(2) The addressee of a data message on which a digital signature is affixed is entitled to regard the data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied the originator's public key to the data message as received and the application of the originator's public key revealed: that the received data message had been encrypted with the originator's private cryptographic key; and that the initial message had not been altered after being encrypted through the use of the originator's public cryptographic key;

or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to the originator's private cryptographic key.

(3) Paragraph (2) does not apply:

(a) as of the time when the addressee knew or should have known, had it sought information from the authorized certification authority or otherwise exercised reasonable care, that the validity of the originator's public cryptographic key had expired, or that the certificate issued by the certification authority had been revoked or suspended;

or

(b) in a case within paragraph (2)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator."

Remarks

65. The Working Group may wish to discuss whether the issue of attribution of digitally signed messages might be dealt with simply by way of a reference to article 13 of the Model Law. Draft article E, which is modelled on article 13 of the Model Law, is intended to provide an illustration of the principles contained in article 13 in the context of digital signatures. It is based on the need to provide certainty as to the legal effect of digital signatures, which are currently regarded as a highly secure authentication procedure. The draft provision places a heavy burden on the originator of a message bearing that originator's digital signature. It may be recalled that, under article 2(c) of the Model Law, "originator" means any person by whom, or on whose behalf, the data message purports to have been sent. The draft provision illustrates the need for any user of a digital signature to protect its private key which, if applied to encrypt a message, will create an irrebuttable presumption that the message was that of the purported originator.

4. Revocation of certificates

66. "Draft article F

(1) The holder of a certified key pair may revoke the corresponding certificate. The revocation is effective from the time when it is [registered][received] by the certification authority.

(2) The holder of a certified key pair is under an obligation to revoke the corresponding certificate where the holder learns that the private cryptographic key has been lost, compromised or is in danger of being misused in other respects. If the holder fails to revoke the certificate in such a situation, the holder is liable for any loss sustained by third parties having relied on the content of messages as a result of the holder's failure to undertake such revocation."

Remarks

67. The Working group may wish to note that, should it be provided in the uniform rules on digital signatures that revocation of a certificate becomes effective at the time when it is received by the certification authority, paragraph (4) of draft article H (liability) might be deleted since there could be no basis for the liability of the certification authority for fault or negligence in the registration of the revocation.

5. Register of certificates

68. "Draft article G

(1) An authorized certification authority shall keep a publicly accessible electronic register of certificates issued, indicating when the individual certificate was issued, when it expires or when it was suspended or revoked.

(2) The register shall be maintained by the certification authority for at least [10] years after the date of revocation or expiry of the operational period of any certificate issued by that certification authority."

Remarks

69. The Working Group may wish to discuss whether a register of certificates should be publicly accessible or whether access to such a register might somehow need to be limited to interested parties. As to the time during which such a register should be maintained, the Working Group may wish to discuss whether any fixed period of time should be provided as a uniform rule, whether determination of that period should be left to the discretion of enacting States, or whether it should attempt to provide a more flexible criterion, e.g., by indicating that the register should be accessible to verify certificates during the operational period of each certificate and until the end of the period of time during which messages digitally signed under the certification authority's certificates would be used or need to be verified, which might make it necessary to provide several time periods, depending on existing laws on limitation and prescription.

6. Liability

70. "Draft article H

(1) An authorized certification authority shall be liable to any person who has acted in good faith in reliance on a certificate issued by the certification authority for any loss due to defects in the registration of the certification authority, technical breakdowns or similar circumstances [even if the loss is not due][if the loss is due] to negligence by the certification authority.

(2) Variant X The liability for any individual loss shall not exceed [amount]. The ... [the enacting State specifies the organ or authority competent to revise the maximum amount] may regulate this amount every second year to reflect price developments.

Variant Y The ... [the enacting State specifies the organ or authority competent to promulgate liability regulations] may promulgate regulations on the liability of certification authorities.

(3) In case the party who has sustained the loss has contributed to this wilfully or negligently, the compensation may be reduced or may not be granted.

[(4) Where an authorized certification authority has received notice of revocation of a certificate, the authority shall register such revocation forthwith. If the authority fails to do so, it shall be liable for any resulting loss sustained by the user.]

Remarks

71. The Working Group may wish to discuss whether a provision on liability should expand to cover cases beyond negligence by the certification authority. The Working Group may also wish to determine whether and to what extent party autonomy should apply to allow certification authorities to control, by private agreement with the users, the extent to which they should be liable.

72. The Working Group may wish to consider including a "safe-harbour" provision along the following lines:

> "A certification authority that complies with [this Law][these Rules] and any applicable law or contract is not liable for any loss which
>
> (1) is incurred by the holder of a certificate issued by that certification authority as a result of the holder's reliance on that certificate, or
>
> (2) is caused by reliance upon a certificate issued by that certification authority, upon a digital signature verifiable through reference to a public key listed in a certificate issued by that certification authority, or upon information represented in such a certificate."

7. Issues of cross-certification

73. "Draft article I

> (1) Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as digital signatures subject to [this Law][these Rules] if they are recognized by an authorized certification authority, and the authorized certification authority guarantees, to the same extent as its own certificates, the correctness of the details of the certificate as well as the certificate being valid and in force.
>
> (2) The ... [the enacting State specifies the organ or authority competent to establish rules in connection with the approval of foreign certificates] is authorized to approve foreign certificates and to lay down specific rules for such approval.

Remarks

74. Draft article I is based on the notion that recognition of foreign certificates should be provided under the responsibility of a local certification authority on the basis of reciprocity. In discussing the issues of cross-certification, the Working Group may wish to consider whether full reciprocity should be required or whether guarantees as to the correctness and validity of foreign certificates might not necessarily be provided at the same level by all authorities that would form part of a cross-certification scheme. The Working Group may also wish to consider whether Government intervention should necessarily be required for recognition of foreign certificates.

75. As a possible alternative to draft article I, the Working Group may consider the approach taken in draft legislation in certain countries, under which recognition of foreign certificates could only be provided on the basis of bilateral or multilateral international agreements.

8. Relations between users and the certification authority

76. "Draft article J

(1) A certification authority is only allowed to request such information as is necessary to identify the user.

(2) Upon request from legal or natural persons, the certification authority shall deliver information about the following:

(a) the conditions under which the certificate may be used;

(b) the conditions associated with the use of digital signatures;

(c) the costs of using the services of the certification authority;

(d) the policy or practices of the certification authority with respect to the use, storage and communication of personal information;

(e) the technical requirements of the certification authority with respect to the user's communication equipment;

(f) the conditions under which warnings are given to users by the certification authority in case of irregularities or faults in the functioning of the communication equipment;

(g) any limitation of the liability of the certification authority;

(h) any restrictions imposed by the certification authority on the use of the certificate;

(i) the conditions under which the user is entitled to place restrictions on the use of the certificate.

(2) The information listed in paragraph (1) shall be delivered to the user before a final agreement of certification is concluded. [That information may be delivered by the certification authority by way of a certification practice statement].

(3) Subject to a [one-month] notice, the user may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received by the certification authority.

(4) Subject to a [three-month] notice, the certification authority may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received.

III. INCORPORATION BY REFERENCE

A. Previous discussion

77. At the twenty-eighth session of the Working Group, a proposal was made to include in the draft UNCITRAL Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication a provision to the effect of ensuring that certain terms and conditions that might be incorporated in a data record by means of a mere reference would be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of the data record. It was stated that the issue of incorporation by reference of certain terms into EDI messages was crucial to EDI users and that there existed an important need for certainty in the use of that method. It was said that, arguably, EDI was inherently a system of incorporation by reference since EDI messages were meaningless, and of little contractual value, without the incorporation by reference of the relevant communication standards. It was decided that the Working Group would address, in the context of a future session, the issue of incorporation of terms and conditions into a data message by means of a mere reference to such terms and conditions (A/CN.9/406, paras. 90 and 178).

78. At its twenty-ninth session, the Working Group had before it two proposals for a draft provision on incorporation by reference, one submitted by the observer for the International Chamber of Commerce (A/CN.9/WG.IV/WP.65) and another submitted by the United Kingdom of Great Britain and Northern Ireland (A/CN.9/WG.IV/WP.66). The prevailing view was that the issue was not mature for inclusion in the Model Law and deserved further study. It was stated that both proposals presented to the Working Group needed to be further clarified on a number of issues, such as what terms would be incorporated and in what circumstances. In addition, it was stated that both proposals might appear as interfering with general rules of contract law. Moreover, it was stated that incorporation by reference in an electronic environment did not need to be addressed in the Model Law since it raised essentially the same issues as incorporation by reference in a paper-based environment, which were dealt with by general contract law. Finally, it was said that a provision distinguishing between incorporation by reference in paper-based and EDI communications would be inconsistent with the approach followed thus far by the Working Group, which was aimed at ensuring "media-neutrality". It was stated, in response, that there was a perception among practitioners that the issue of incorporation by reference was more complex in EDI than in a paper-based environment, for example because the number of communications involved was larger and terms incorporated by reference might be more difficult to ascertain if they were in the form of data messages. There also existed a perceived need among practitioners for specific provisions dealing with incorporation by reference in the context of electronic communications. Another point was that, in view of the number of data messages involved in a particular contractual relationship conducted through EDI, the problem known as the "battle of forms" was particularly likely to arise in the context of electronic communications. The Working Group agreed that the issue of incorporation by reference might need to be further considered in the context of future work (A/CN.9/407, paras. 100 to 105 and 117).

79. At its thirtieth session, the Working Group was generally agreed that work with respect to incorporation by reference in the context of EDI was needed. The view was expressed that, in any attempt to establish legal norms for such incorporation of reference clauses in data messages, the following three conditions should be met: (1) the reference clause should be inserted in the data message; (2) the document being referred to, e.g., general terms and

conditions, had actually to be known to the party against whom the reference document might be relied upon; and (3) the reference document had to be accepted, in addition to being known, by that party. It was generally agreed that the topic of incorporation by reference would appropriately be dealt with in the context of more general work on the issues of registries and service providers (A/CN.9/421, para. 114). The Commission, at its twenty-ninth session, was generally agreed that the issue could be dealt with in the context of work on certification authorities (A/51/17, para. 222).

B. Possible need for uniform rules on incorporation by reference

80. Incorporation by reference is a concise means of referring generically in a document to provisions which are detailed elsewhere, rather than reproducing them in full. For example, it makes it unnecessary to set out lengthy standards terms when negotiating or concluding contracts. The terms may thus be read into the document or data message which refers to them, simply by the device of identifying the terms sufficiently and indicating an intention to include them. In an electronic environment, incorporation by reference may be defined as the method of making one data message or record (or part of the information contained therein) become a part of another separate data message or record by referring to the former in the latter, and declaring that the former shall be taken and considered as a part of the latter as if it were fully set out therein.

1. Traditional rules developed in a paper-based environment

(a) Incorporation by reference

81. The legal issues raised by incorporation by reference are known in the context of paper-based communications, and legal rules exist in many legal systems, establishing the legal conditions under which information which is not fully expressed in a written document may legally be regarded as part of that document. For example, under certain conditions, a reference to one or more INCOTERMS, such as "carriage paid to" (CPT) or "carriage and insurance paid to" (CIP), may be included in a purchase order or in an invoice, with the consequence that those INCOTERMS will be regarded as one of the terms of the corresponding sales contract without the actual definition of "CPT" or "CIP" sales being stated in full in any of the contractual documents. The incorporation by reference of the INCOTERMS may be facilitated by the fact that such terms were prepared by the International Chamber of Commerce (ICC) specifically for inclusion into contracts through the use of their acronyms or abbreviated designations, which are widely known and recommended for use both by the ICC and by UNCITRAL. Another example of a text which is often incorporated by reference is the Uniform Customs and Practice for Documentary Credits (UCP 500) prepared by the ICC. The legal reasoning used for allowing a text such as the UCP 500 to be incorporated by reference into a contract would often be based on the recognition that such a text records widely known and accepted practice worldwide, and is presumed to be known by all parties involved.

82. Where no such presumption applies, the conditions set forth by national law for validating incorporation by reference may involve strict requirements, such as actual knowledge of the information incorporated by reference by all parties, or even express approval of that information by the party against whom enforcement is sought. Under certain national laws, however, the requirements for validating incorporation by reference are more lenient. For

example, certain traditional legal tests of incorporation by reference may focus on the clarity of the clause by which incorporation by reference is effected and on the accessibility of the information incorporated by reference.

(b) "Battle of forms"

83. The issue of incorporation by reference is not to be confused with the issue generally known as the "battle of forms". A battle of forms may occur where, for example, the general contracting terms and conditions proposed by a buyer are stated in small print on the back of its purchase order, while a different set of general contracting terms and conditions is stated on the back of the invoice issued by the seller. Where no specific agreement has been entered into by the buyer and the seller as to which terms and conditions will apply to a given contract, and two conflicting sets of terms and conditions have been communicated by the parties on the back of their contractual documents, there may be a need to solve the uncertainty as to which terms and conditions will govern the transaction. In many countries, legal rules of contract law have been developed for the purpose of solving that ambiguity.

2. Issues raised in an electronic commerce environment

(a) Widespread use of incorporation by reference

84. Incorporation by reference is essential to widespread use of electronic data interchange (EDI), electronic mail, digital certificates and other forms of electronic commerce. For example, communications by way of standard EDI messages, and electronic communications in general, are typically structured in such a way that large numbers of messages are exchanged, with each message containing brief information, and relying much more frequently than paper documents on reference to information accessible elsewhere. EDI and other highly structured and formatted types of data invariably make extensive use of incorporation by reference to enhance the efficiency of data processing. At previous sessions of the Working Group, it was stated that EDI and diverse forms of electronic commerce were fundamentally systems of incorporation by reference. As a practical matter, EDI messages are potentially less legally certain unless clarity is provided as to the validity and effectiveness of the incorporation by reference of the relevant legal, technical, and administrative terms, conditions, clauses, agreements, standards, rules, or guidelines that may be applicable to those messages.

85. With respect to situations where a "battle of forms" would occur in a paper-based environment, it should be borne in mind that electronic messaging is not intended and not even equipped to transmit with each message texts such as general terms and conditions typically printed on the back of paper documents. The inclusion of all relevant terms and conditions would be expensive and inefficient. It would slow down and perhaps stall electronic communication, and might even reduce the effectiveness of notice by forcing relying parties to either print or scroll through such lengthy text. Developing rules as to how such texts might be regarded as incorporated into a message is thus necessary. The aim of such rules, if possible, should be to reduce in an electronic environment the difficulties that result from a battle of forms in a paper-based environment or, at least, to ensure that the solutions elaborated under many national laws to solve those difficulties in a paper-based environment would also be available in an electronic environment. It should be noted that developing such rules would not necessarily involve changing the solutions that may derive from existing national law as to how a "battle of forms" situation may be solved.

86. Standards for incorporating data messages by reference into other data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size. The trusted third party which issues the certificate, however, is likely to require the inclusion of relevant terms limiting its liability. The scope, purpose and effect of a certificate in commercial practice, therefore, would be ambiguous and uncertain without external terms being incorporated by reference. This is the case especially in the context of international communications involving diverse parties who follow varied trade practices and customs.

87. It has been repeatedly stated at previous sessions of the Working Group that the establishment of standards for incorporating data messages by reference into other data messages was critical to the growth of a computer-based trade infrastructure. Without the legal certainty fostered by such standards, computer-based trade transactions would become burdened by the inclusion of large quantities of material, thereby becoming unwieldy for the parties involved as well as for the system facilitating the transaction. Without such uniform standards, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms. For example, certain traditional legal tests of incorporation by reference may inquire whether the incorporated terms are "clear and conspicuous", whether they contain "suitable words of reference evidencing explicit intention to incorporate", or whether the intended incorporation is "clear and convincing". Such tests may create unintended barriers to the facilitation of electronic trade. Specific rules may be needed because the methods used for giving notice and ensuring access to information may differ in a paper-based environment and in electronic commerce, with the possible consequence that, in some jurisdictions, traditional rules on incorporation by reference might lead to unjustified discrimination against electronic commerce.

(b) Accessibility of incorporated text

88. Electronic commerce relies heavily on the mechanism of incorporation by reference. At the same time, however, the accessibility of the full text of the information being referred to may be considerably improved by the use of electronic communications. For example, a message may have embedded in it uniform resource locators (URL), which direct the reader to the referenced document. Such URLs can provide "hypertext links" allowing the reader to simply direct a pointing device (such as a mouse) on a key word associated with a URL and the referenced text would appear.

89. The same methods may be used in an electronic environment for ensuring easy access of all users to a variety of texts, such as: (1) texts embodying established commercial practice (e.g., UCP 500); (2) technical standards governing the communication; (3) certification practice statements issued by certification authorities; and (4) more specific information such as a company's general contracting terms and conditions. The legal effect of these methods, however, cannot be confidently relied upon without standards for incorporating data messages by reference into other data messages.

90. The need for development of rules on incorporation by reference in an electronic environment results both from the frequency at which data messages refer to information

recorded elsewhere and from the availability of the technical means that make verification of such information easier and quicker than in a paper-based environment.

C. Possible provisions

91. In developing possible provisions on incorporation by reference in electronic commerce, the Working Group may wish to bear in mind that, in certain jurisdictions, the existing rules developed for use in a paper-based environment are based on the concern that the terms or other information incorporated should be properly brought to the notice of the addressee, or a third party, as the case may be. Where such rules of law exist, it may be appropriate for them to apply irrespective of whether the incorporation by reference is made by means of EDI or by any other type of communication.

92. It would nevertheless seem possible to formulate a general principle clarifying that incorporation by reference is effective in electronic commerce, provided that it is also made clear that this principle does not affect any rules which may exist relating to: (1) the need for the content or location of the terms or other information to be brought to the attention of any party to whom they are to apply, or to be available to that party; or (2) any legal requirement that terms should be accepted before they can form part of a contract. The essential principle is that the use of incorporation by reference should be recognized, so that the fact that information is only set out elsewhere does not in itself prevent that information from being read into the data message in which it is referred to.

93. The Working Group may wish to resume its consideration of the issues of incorporation by reference on the basis of the two following variants:

Variant A

Unless otherwise agreed, when [adequately][reasonably] accessible terms, conditions, clauses, agreements, standards, rules or guidelines are referenced in full or in part in a data message with the [apparent] intent to incorporate them as part of the content or otherwise to be legally binding, those terms shall be presumed to be incorporated by reference in that data message. Between the parties, such terms shall be as legally effective and binding as if they had been fully stated in the data message, to the extent permitted by law.

Variant B

(1) This article applies where information recorded or communicated in a data message refers, or is only fully ascertainable by reference, to information recorded elsewhere ("the further information").

(2) Subject to paragraph (4), the data message shall have the same effect as if the further information were fully expressed in the data message, and ascertainable solely by reference thereto, if the data message:

(a) identifies the further information:

(i) by a collective name or description; and

(ii) by identifying the record, and the parts of that record, containing the further information, and, where that record is not publicly available, the place where it may be found; and

(b) expressly indicates or carries a clear implication that the data message should have the same effect as if the further information were fully expressed in the data message.

(3) Nothing in this article affects:

(a) any rule of law which requires adequate notice to be given of the content of the information recorded elsewhere, or of the record or place where such information may be found, or which requires that record or place to be accessible to another person; or

(b) any rule of law relating to the acceptance of an offer for the purpose of contract formation.